UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/551,397	07/07/2006	Salvatore E. Scottodiluzio	PATH 3822003	3268

21909 7590 07/18/2008

CARR LLP
670 FOUNDERS SQUARE
900 JACKSON STREET
DALLAS, TX 75202

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
07/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/551,397	SCOTTODILUZIO, SALVATORE E.	
	Examiner	Art Unit	
	LONGBIT CHAI	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 September 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/23/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 9/29/2005 but is a 371 case of PCT/US04/09682 application filed 3/30/2004 and has a U.S. provisional application number 60/459,720 filed on 4/2/2003.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 – 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yanovsky (U.S. Patent 5,703,948), in view of Rodriguez et al. (U.S. Patent 7,209,559).

As per claim 1, Yanovsky teaches a method for secure data transmission using multiple encryption keys comprising:

dividing a message object to be encrypted into a plurality of portions, each portion being associated with a shift point (Yanovsky: Figure 1 & Column 2 Line 42 – 55 and Column 4 Line 44 – 55);

utilizing a first key to encode a first portion of the message object (Yanovsky: Figure 1 & Column 2 Line 42 – 55);

when a first shift point occurs, generating a second key by executing a function that uses the first key and additional information (Yanovsky: Figure 1 & Column 4 Line 45 – 49 and Column 7 Line 61 – 65: as shown in Figure (1), the current encryption key K_E generated by the transmitter (TR) is feedback to the Normal State Machine (NSM) to generate the next / subsequent key);

utilizing the second key to encode a second portion of the message object (Yanovsky: Figure 1 & Column 2 Line 42 – 55);

upon completion of encoding of all of the plurality of portions of the message object, transmitting the encrypted message object to a receiver (Yanovsky: Column 2 Line 42 – 55).

However, Yanovsky does not teach destroying the keys.

Rodriguez teaches destroying the keys (Rodriguez: Column 7 Line 20 – 21).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rodriguez within the system of Yanovsky because (a) Yanovsky teaches protecting communication data based on the usage of dynamic random keys (Yanovsky: Column 2 Line 30 – 41), and (b) Rodriguez teaches an enhanced security mechanism by destroying the encryption keys once the content / data message is encrypted (Rodriguez: Column 7 Line 20 – 21).

As per claim 2, Yanovsky as modified teaches when each subsequent shift point occurs, generating a subsequent key by executing the function using a current key and additional information; and utilizing the subsequent keys to encode subsequent portions of the message object (Yanovsky: Figure 1 & Column 4 Line 45 – 49 and Column 7 Line 61 – 65: as shown in Figure (1), the encryption key K_E generated by the transmitter (TR) is feedback to the Normal State Machine (NSM) to generate the next / subsequent key).

As per claim 3, Yanovsky as modified teaches at least a portion of the additional information to the receiver for decoding of the encrypted message, wherein the portion of the additional information comprises a password and shift points (Yanovsky: Column 15 Line 63 – Column 16 Line 21 and Column 4 Line 60 – 61: an one-time PAD is qualified as a password and the associated process indeed affects the generation of the encryption keys based on the synchronization conditions).

As per claim 4, Yanovsky as modified teaches the additional information comprises a password, an iteration value, and a symbol value, and the function executed is a hash algorithm (Yanovsky: Column 15 Line 63 – Column 16 Line 21, Column 5 Line 33 – 35, Column 4 Line 60 – 61 and Column 8 Line 9 – 11: (a) an one-time PAD is qualified as a password and the associated process indeed affects the generation of the encryption keys based on the synchronization conditions (b) a counter defined by a predetermined number of rounds is qualified as an iteration value (c) random-bits is qualified as a symbol value and (d) a function which is not permitting the inputs to be determined by the outputs is qualified as a hash function).

As per claim 5, Yanovsky as modified teaches the first key is a piece of digital media (Yanovsky: Figure 1 & Column 2 Line 42 – 55 and Column 4 Line 44 – 55: a media is interpreted as a means of communications such as data).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.
Patent Examiner
Art Unit 2131
7/8/2008